



# Jefferson Science Associates

**Thomas Jefferson National Accelerator Facility**

July 1, 2008

Dear Colleagues:

We must all maintain the highest standards in our stewardship of government property, information, and technology. While we have policies and procedures in place to protect property, control access to facilities, and protect our electronic systems as a prudent business practice, we need to review and update the fundamentals of Jefferson Lab's security program regularly.

It is Jefferson Lab policy to pursue its scientific mission in both a safe and secure manner. Security is managed in the same integrated manner as safety, and your personal knowledge and commitment are essential. We all have the responsibility to carry out our work in a secure manner, adhering to all applicable policies and procedures and being alert to any potential for security breach at the laboratory. While we have administrative and engineered controls in place, experience shows that the very best insurance of a secure workplace is an alert, informed and engaged staff and I encourage you to accept the personal responsibility for updating your understanding and awareness of Jefferson Lab's security policies and procedures.

Information regarding responsibilities for physical security is found at [http://www.jlab.org/div\\_dept/train/lms/security\\_awareness/2008/index.html](http://www.jlab.org/div_dept/train/lms/security_awareness/2008/index.html) and policies and tips regarding constantly-changing cybersecurity threats can be found at <http://cc.jlab.org/policies>.

Another vital security area is Export Controls, designed to protect items and information important to the United States. Be sure you understand export-control requirements related to your work and ensure no exports are made contrary to federal law since noncompliance could result in administrative or criminal penalties for the Lab and/or you. The Property Office and Export Control office are valuable resources for these issues. I would also remind you that Jefferson Lab property and equipment are to be used only for official JLab business and you should report any unauthorized use of JLab property to your supervisor; the Security office; or the Fraud, Waste & Abuse reporting line (757-269-7137).

This message is a reminder of the duty each of us has in maintaining a secure work environment. I expect you to complete the revised Security Awareness refresher training as soon as it is posted each new calendar year. Also take time on a regular basis to review your responsibilities in the area of security and if you are uncertain how to handle any security-related matter, call the JLab Security office at ext. 7169 or after hours call Guard Post 2 at ext 5822. For additional information, visit <http://www.jlab.org/intralab/security/>.

Sincerely,

Christoph W. Leemann  
JSA President  
Director, Jefferson Lab